Concept for High-Survivability, High-Security Orbital Communications Relay System Including Perpetually Wandering Non-GSO HEO Master Relays

16 August 2023
Simon Edwards
Research Acceleration Initiative

Introduction

In a geopolitical climate in which foreign attempts at the disabling of domestic civilian and military communications systems are no longer a question of 'if', but 'when,' any novel communication relay system, to be useful in a maximally contested condition, must bring to bear the latest available technologies to increase its survivability and protect the security of the data it is designed to relay.

There are a number of features that a next-generation platform for satellite-based communication might employ to enhance survivability and data security whilst attenuating the detectability of both the platform itself as well as its emitted electromagnetism.

Abstract

The technology now exists to enable LASER-based communications between orbital platforms via add-on modules affixed, overtly or covertly, to existing military and commercial platforms. Collimated LASERs have already been demonstrated that are capable of relaying data securely between these add-on modules so as to create alternative data routing options for orbital platforms and to enable the operation of a variety of clandestine platforms without require the emission of microwave-band energy that would expose the platform's position.

Taking this albeit pre-existing concept a step further, provided that these modules are affixed to virtually all orbital platforms, they might be used on a routine basis rather than on an emergency basis. With so many routing options, data might be transmitted, in addition to any encryption employed, in piecemeal fashion with packets alternatively being transmitted through different pathways as part of the network's default mode of operation.

Transmitting packets in this manner would frustrate attempts at intercept which, as things already stand, require that an intercept platform be positioned directly between two communicating LASER-based modules. Data may, in addition to being encrypted, be transmitted in an out-of-sequence fasion according to a pre-determined system that would frustrate any attempt at cryptanalysis.

Out-of-Sequence Encrypted Data Transmission/Dynamical Beam Redirection for Consistent Trans-Platform Lock

Relays may hold data in reserve according to a pre-established set of rules, ultimately transmitting a packet received first, last, i.e. scrambling. Given the constant movement of LEO orbital platforms, a mechanism is required to enable these platforms to maintain a collimated LASER lock on the modules affixed to the other platforms. The same mechanism that can facilitate this can also be used to govern when a data packet is shuffled as part of a scrambling system designed to be superimposed over existing encryption.

A prism of the same sort used to transmogrify single-mode LASER light into a broad range of frequencies in support of LiDAR can be used to inform a LASER receiving system of the angular momentum of inbound light. As each small portion of a dome-shaped prism would modify the frequency of light uniquely, a platform receiving LASER telemetry would know from what angle is beam is being received and, if the receiver is about to stray out of the scope of the beam, can send a signal to the module generating the signal informing that module to alter the direction of the transmission accordingly. This is necessary for enabling a network of collimated LASERs to maintain situational awareness with regard to the location of other platforms while maintaining radio silence.

These prisms could be imbued with features that are unique to each unit sc. a small area of the dome-shaped prism that, when struck by a beam head-on, triggers a shuffling mechanism that results in the relay of a single packet in an out-of-sequence fashion. Any relay in the network may or may not perform a shuffle according the angle from which LASER data was received. As the specific properties of the prisms installed on the orbital platforms are, in theory, known only to the nation that deploys them, only the authentic recipient of the data would know how to unscramble the received data prior to performing decryption. The de-scramble operation would be based upon a closed-source program that takes into consideration the exact time of transmission and the predicted position of all orbital platforms in order to discover when the "sweet spot" of the prism might be struck head-on, triggering a shuffle operation.

In this way, the compromise of the firmware driving the SATCOM platforms would not necessarily lead to the compromise of the transmitted data as at least a portion of the encryption would be based upon the properties of a piece of hardware not tied to any software.

Non-Geosynchronous HEO Master Relays: Protecting the Weak Link

SATCOM relay systems that facilitate global communications are traditionally emplaced in fixed, known positions in High-Earth Orbit. These platforms, although they can be moved, can oftentimes, when emitting microwave-band energy, be relocated by a hostile nation in short order. Next-generation systems, given that they do not utilize microwave-band EM, may be successfully hidden from an enemy if the platform is kept constantly in motion.

By equipping the HEO platforms with ionic thrusters, these platforms may wander about in HEO, slowly moving in a stochastic, gradual, pre-programmed

fashion into different positions whilst always maintaining an identical relative position to the others. These sorts of platforms are usually launched in threes as three relays are sufficient to maintain line-of-sight between the platforms whilst enabling ground stations to ultimately communicate with these platforms.

While these HEO relays have, in the past, been communicated with directly by broadcast microwave emissions from ground stations, the modern military version of these platforms would, by design, not be reachable in this manner. These platforms would only accept LASER-based communication from LEO platforms, with collimated microwaves being used to communicate with covert LEO platforms that route their traffic by LASER to other LEO platforms to mask the position of these covert platforms with data being routed to the HEO platforms only after making several hops through LEO satellite modules.

High-powered collimated LASER communication would facilitate communication between the HEO platforms. Data, once relayed to the distant HEO platform could be sent downstream to LEO modules over our own hemisphere and from there, to covert LEO platforms emitting collimated microwaves that may be collected at a ground station in friendly territory.

Conclusion

Although apparently intricate, the technology to create a network that operates according to these principles already exists thus, this concept may be readily realized in order to create a HEO SATCOM relay system of a qualitatively higher order.